[National Cyber Security Centre Annual Review 2021 Launch](#)

As the Government's lead minister for cyber, I'm delighted to be here for the launch of the NCSC's Annual Review.

Its pages tell the story we have come to expect from an organisation whose impact on the nation's cyber security – in just five years – has been profound.

As the Review shows, the NCSC responded with speed and strength to keep our country safe in cyberspace.

Our cybersecurity colleagues followed the risk wherever it took them:

whether it was to defend UK consumers from internet scams,

or to defend our COVID research, our stocks of vaccines, or our vaccine rollout from threats.

It is a story of protection and of innovation –

of decisive action against the criminals who attack government networks and citizens –

and of delivering for the United Kingdom and our partners across the globe.

The pandemic pivot

As has been the case for all of us, the pandemic has continued to dominate the NCSC's recent activities.

At a time of great national uncertainty, the technology in which the NCSC specialises has allowed millions of people to work and learn remotely

for MPs like me to take part in virtual House of Commons debates and to vote online; and concerned citizens to seek out information about the COVID-19 virus itself.

But this dramatic shift online has also tempted criminals – who use cyber technology for black arts – to try to scam millions of individuals and businesses.

In particular, they have preyed on peoples' worries about the virus, at a time when they felt most vulnerable.

Countless attempts have been made to lure people into handing over bank details by charging for fake vaccine appointments; or for sought-after items that were at the time in short supply, such as personal protective equipment or essential household goods.

And we see all this reflected in the Annual Review.

The NCSC's Active Cyber Defence programme has the clear aim of keeping the public and organisations safe at scale, underpinned by its vow to 'Protect the majority of people in the UK, from the majority of the harm caused by the majority of the cyber attacks, the majority of the time' .

This year, it has taken down no fewer than 2.3 million cyber-enabled 'commodity campaigns' — that's the unsophisticated, but effective, off-the-shelf 'spoofing' scams that are easy for low-level criminals to post on the internet.

These included 442 phishing campaigns that used NHS branding; and 80 illegitimate NHS apps that were available to download outside official app stores.

The worried public has also played its part in keeping itself safe.

People have been inundating the innovative Suspicious Email Reporting Service, or 'SERS', which NCSC established in April 2020.

In total, SERS has received more than eight million reports, of which nearly six million have come in this year alone. As a result, more than 67,000 scam operations have been taken down.

Fighting cyber crime together

And I am truly heartened by the heightened awareness that this shows of the fraudsters operating in our midst.

While the NCSC never stops in its efforts to protect citizens and businesses — and has consistently pioneered new ways to make the UK the safest place to live and work online — there are ways that we can, as a united team, defend ourselves against the scammers and fraudsters.

The success of the NCSC in pushing the potential of technology and the Digital Age has been recognised by industry and governments around the world. It is firmly established in the UK, and is of course a vital part of our cyber defences.

Yet cyber security is, and always will be, a team sport.

Across government, a range of departments play their part: including Cabinet Office, the Treasury, the Foreign Commonwealth and Development Office, the Home Office, and the Department for Digital, Culture, Media and Sport.

Cyber was also prominent in the recently-published Integrated Review, at the heart of our national and international strategy: with the Government determined to ensure that the UK is a leading, responsible, democratic, cyber power.

Even so, the UK's cyber security team is — must be — much bigger than government alone.

From business and law enforcement to academia and the cyber security industry – and of course individual members of the public – there are many links in the strong chains that keep us safe.

And what I have already learned about cyber security is that there is never a 'one and done' moment. The NCSC is always improving and learning; strengthening and reinforcing those chains.

The next five years and beyond

And for the NCSC and for all cyber stakeholders, 2021 is a landmark moment because it is the end of the UK's ground-breaking five-year cyber security strategy. At such time, we should evaluate some extraordinary progress, and look ahead to the new National Cyber Strategy that we will be publishing in the near future.

This will broaden our approach beyond cybersecurity alone, setting out how the UK will expand as a leading international cyber power by considering the full range of capabilities, including the newly established National Cyber Force.

It will highlight how we will protect and promote our interests in and through cyberspace, staying ahead of our adversaries and detecting, disrupting and deterring their malign activities.

It will show how we will influence and unlock tomorrow's technologies and opportunities, so they are safe, secure and open.

And it will set out how we will deepen our support for the public to be safe and secure online.

At its core, the new strategy will take a 'whole of society' approach to cyber: government working in partnership with industry and the public; a cyber sector growing within our economy; and critical national infrastructure more able to withstand threats from hostile states.

The Budget last month and the Spending Review reflect the Government's commitment to this critical area. The National Cyber Security Programme budget was increased by £114 million and we are investing £2.6 billion in cyber and legacy IT over the next spending review period.

In the coming years, we must of course be alive to the risks posed by cyberspace, but we must also be poised to take advantage of the fantastic opportunities the digital age presents.

Cyber and levelling up

And as a Lancastrian, I am delighted that the newly launched National Cyber Force will be located in Samlesbury near Preston – delivering investment and driving economic growth across the North West. This is just one example of how we can use cyber to drive positive change and link to our levelling up agenda.

Another positive change driven by cyber is in delivering our ambition for the UK to be a Science and Tech superpower, building on the increase in R&D spend from £15 billion to £20 billion this Parliament.

With technology continuing to develop at a rapid pace, the UK must be at the forefront of research and development – as well as play an important role in global regulation on technology, cyber, digital and data. This will help bolster the UK's status as a global services, digital and data hub, maximising the commercial and employment opportunities for the British people.

Five years in, the NCSC has come a long way – but there is always so much more to do, to keep a step ahead of the cyber criminals. Over the coming years, we must build on our successes, without ever being complacent about the challenges that we face.

And I look forward to working with you, Lindy, and colleagues in and outside government as we seek to confront these challenges.

Thank you very much.